

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
TEXARKANA DIVISION**

DEXON COMPUTER INC.
Plaintiff

V.

**CISCO SYSTEMS, INC. and
CDW CORPORATION**
Defendants

§
§
§
§
§
§
§
§

**Civil Action No. 5:22cv53-RWS-JBB
SEALED**

ORDER

The above-referenced cause of action was referred to the undersigned United States Magistrate Judge for pretrial purposes in accordance with 28 U.S.C. § 636. The following motion is pending before the Court:

Dexon Computer Inc.’s *Daubert* Motion to Exclude Opinions of Richard LaMagna (Dkt. No. 330).

Dexon’s motion is **GRANTED IN PART and DENIED IN PART**. The Court grants Dexon’s motion to exclude LaMagna’s opinions that Cisco’s brand protection practices are consistent with the practices of other manufacturers of networking equipment; otherwise, Dexon’s motion is denied.

I. BACKGROUND

On April 27, 2022, Plaintiff Dexon Computer, Inc. (“Dexon”) filed the above antitrust case against Defendants Cisco Systems, Inc. (“Cisco”) and CDW Corporation (“CDW”) (collectively, “Defendants”). Dexon moves under Federal Rule of Evidence 702 and *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579 (1993), to exclude twenty-four paragraphs (out of a total of

approximately 227 paragraphs) of the expert reports of Richard LaMagna, Defendants’ proffered expert on brand protection and anti-counterfeiting.

In his opening report, LaMagna (1) explains the business justifications and purposes of brand protection programs, Dkt. No. 330-2 (LaMagna Opening Report), ¶¶ 15, 31-53; (2) analyzes Cisco’s brand protection policies and practices, which include agreements with channel partners, counterfeit-detection tools, and educational and enforcement efforts, and concludes Cisco’s brand protection policies and practices are “consistent with brand-protection best practices, aligning with the multifaceted brand-protection program [LaMagna] designed at Microsoft and the practices of other networking-equipment manufacturers,” *id.*, ¶¶ 15, 54-86; and (3) analyzes Dexon’s purported “anticounterfeiting measures” and concludes those measures are “inadequate” to “prevent Dexon from supplying customers with counterfeit ‘Cisco’ products.” *Id.*, ¶¶ 15, 87-124.

In its *Daubert* motion, Dexon does not challenge LaMagna’s experience or qualifications as a brand protection expert,¹ or his opinions regarding the business justifications and purposes of brand protection programs or Cisco’s brand protection policies and practices. *See* Dkt. No. 330 at 7 (“While LaMagna’s experience may qualify him to provide general testimony regarding brand protection, LaMagna goes beyond that in opining that Cisco’s brand protection and anti-counterfeit measures are consistent with the networking industry at large.”). Rather, Dexon challenges two discrete parts of LaMagna’s analysis, that (i) Dexon has sold purported counterfeit “Cisco” products; and (ii) Cisco’s brand protection practices are consistent with those of other

¹ LaMagna has spent more than twenty-eight years in law enforcement investigating international organized crime with the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration (DEA) and assisting the National Security Council. LaMagna also has worked with more than a dozen companies, including high-tech companies, to develop and implement brand protection and anti-counterfeiting programs. In the late 90s and early 2000s, LaMagna served as the Director of the Microsoft Global Anti-Counterfeiting Team. Dkt. No. 330-2 (LaMagna Opening Report), ¶ 8. For five years, LaMagna helped build, develop, and manage Microsoft’s brand protection and anti-counterfeiting team, after which time he became the Director of Global Law Enforcement Training and Outreach at Microsoft Legal from 2004 to 2006. *Id.*, ¶ 10.

manufacturers of networking equipment. Dkt. No. 349 at 1. Specifically, Dexon summarizes its two complaints as follows:

LaMagna is not an engineer and admitted at his deposition that his opinions simply repeat the purported counterfeit findings of the Cisco-employee brand engineers that he defers to. **[1] LaMagna is not qualified to provide an opinion here as to whether or not Dexon has sold counterfeit products. [2] Similarly, there is no evidentiary proof to support LaMagna’s conclusions that Cisco’s brand protection practices are consistent with those in the networking industry, as a whole.**

Dkt. No. 330 at 3 (emphasis and numbering added).

II. APPLICABLE LAW

Rule 702 of the Federal Rules of Evidence governs the admissibility of expert testimony and provides as follows:

If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods to the facts of the case.

FED. R. EVID. 702. In accordance with Federal Rule of Evidence 104(a), when faced with expert testimony, the trial court acts as a “gatekeeper” and must perform “a preliminary assessment of whether the reasoning or methodology underlying the testimony is scientifically valid and of whether that reasoning or methodology properly can be applied to the facts in issue.” *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 592–95 (1993).

Prior to admitting expert testimony, “[d]istrict courts must be assured that the proffered witness is qualified to testify by virtue of his ‘knowledge, skill, experience, training, or education.’” *Robison v. Cont’l Cas. Co.*, No. 1:17-CV-508, 2022 WL 336900, at *2 (E.D. Tex. Jan. 6, 2022) (quoting *Wellogix, Inc. v. Accenture, L.L.P.*, 716 F.3d 867, 881 (5th Cir. 2013) (quoting *Wilson v. Woods*, 163 F.3d 935, 937 (5th Cir. 1999)), *cert. denied*, 573 U.S. 904 (2014)).

Accordingly, “[t]o qualify as an expert, ‘the witness must have such knowledge or experience in [his] field or calling as to make it appear that his opinion or inference will probably aid the trier in his search for truth.’” *Id.* (quoting *United States v. Hicks*, 389 F.3d 514, 524 (5th Cir. 2004) (quoting *United States v. Bourgeois*, 950 F.2d 980, 987 (5th Cir. 1992)), *cert. denied*, 546 U.S. 1089 (2006)).

Many factors bear on the inquiry into the reliability of scientific and other expert testimony. *Pipitone v. Biomatrix, Inc.*, 288 F.3d 239, 244 (5th Cir. 2002) (citation omitted). The four factors identified in *Daubert* form the starting point of the inquiry into the admissibility of expert testimony.² *Id.* at 245. However, as the Supreme Court noted in *Kumho Tire*, “the factors identified in *Daubert* may or may not be pertinent in assessing reliability, depending on the nature of the issue, the expert’s particular expertise, and the subject of his testimony.” *Id.* (quoting *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 150, 119 S.Ct. 1167 (1999)). It is a fact-specific inquiry. *Id.* The Advisory Committee notes to Rule 702 provide as follows:

When facts are in dispute, experts sometimes reach different conclusions based on competing versions of the facts. The emphasis in the amendment on “sufficient facts or data” is not intended to authorize a trial court to exclude an expert’s testimony on the ground that the court believes one version of the facts and not the other.

Id. at 249.

The court’s analysis focuses on the reasoning or methodology employed by the expert, not the ultimate conclusion. *Watkins v. Telsmith, Inc.*, 121 F.3d 984, 989 (5th Cir.1997). The purpose being “to make certain that an expert, whether basing testimony upon professional studies or

² In *Daubert*, the Supreme Court offered an illustrative, but not an exhaustive, list of factors that district courts may use in evaluating the reliability of expert testimony. *Pipitone v. Biomatrix, Inc.*, 288 F.3d 239, 244 (5th Cir. 2002) (citation omitted). These factors include whether the expert’s theory or technique: (1) can be or has been tested; (2) has been subjected to peer review and publication; (3) has a known or potential rate of error or standards controlling its operation; and (4) is generally accepted in the relevant scientific community. *Id.*

personal experience, employs in the courtroom the same level of intellectual rigor that characterizes the practice of an expert in the relevant field.” *Skidmore v. Precision Printing and Packaging, Inc.*, 188 F.3d 606, 618 (5th Cir.1999) (quoting *Kumho Tire*, 119 S.Ct. at 1176). Thus, the court “must review only the reasonableness of the expert’s use of such an approach, together with his particular method of analyzing data so obtained, to draw a conclusion regarding the specific matter to which the expert testimony is directly relevant.” *American Tourmaline Fields v. International Paper Co.*, 1999 WL 242690 at *2 (N.D. Tex. Apr.19, 1999) (citing *Kumho Tire*, 119 S.Ct. at 1177).

As a general rule, questions relating to the bases and sources of an expert’s opinion affect the weight to be assigned that opinion rather than its admissibility. *See* FED. R. EVID. 702 Advisory Committee’s Notes, 2000 Amendments (citing *Rock v. Arkansas*, 483 U.S. 44, 61 (1987)). While the district court must act as a gatekeeper to exclude all inadmissible expert testimony, “the rejection of expert testimony is the exception rather than the rule.” FED. R. EVID. 702 Advisory Committee’s Notes (2000) (citing *Daubert*, 509 U.S. 579; *Kumho Tire*, 526 U.S. 137). Importantly, in a jury trial setting, the court’s role under *Daubert* is not to weigh the expert testimony to the point of supplanting the jury’s fact-finding role; rather, the court’s role is limited to that of a gatekeeper, ensuring that the evidence in dispute is at least sufficiently reliable and relevant to the issue before the jury that it is appropriate for the jury’s consideration. *See Micro Chem., Inc. v. Lextron, Inc.*, 317 F.3d 1387, 1391-92 (Fed. Cir. 2003) (applying Fifth Circuit law) (“When, as here, the parties’ experts rely on conflicting sets of facts, it is not the role of the trial court to evaluate the correctness of facts underlying one expert’s testimony.”).

III. DISCUSSION

A. LaMagna's opinions regarding purported counterfeit products sold by Dexon (LaMagna Opening Report at 6, ¶¶ 88, 117-123; LaMagna Reply Report, ¶¶ 75, 96-97)

1. Challenged opinions

In his opening report dated July 29, 2023, LaMagna opines – without challenge – that Dexon's practices related to the procurement and inspection of purported "Cisco" equipment are inadequate to detect and avoid the trafficking of counterfeit equipment. LaMagna Opening Report, ¶ 87. However, Dexon moves to exclude LaMagna's opinions that the inadequacy of Dexon's anti-counterfeiting measures is confirmed by evidence showing that Dexon has sold counterfeit "Cisco" products repeatedly.³ *See, e.g.*, LaMagna Opening Report, ¶ 88, *see also id.*, ¶ 117 (stating "Dexon has never detected a counterfeit 'Cisco' product yet has sold counterfeit networking equipment repeatedly"). Citing numerous Cisco documents in this case, LaMagna offers the following specific opinions of purported counterfeit Dexon-sold products, all of which Dexon moves to exclude:

118. In order to be considered effective, anti-counterfeiting measures must be able to detect counterfeit products. Yet according to Dexon's witnesses, the measures that it employs have never detected a counterfeit "Cisco" product, even though Dexon acknowledges that such products are pervasive in the marketplace. Dexon acknowledges that it cannot detect counterfeit products. For example, Roush

³ In surrounding paragraphs that Dexon does not challenge, LaMagna explains that Dexon's procurement practices exacerbate the risk that Dexon will buy counterfeit products. *See* LaMagna Opening Report, ¶¶ 96-109. According to LaMagna, Dexon purchases "Cisco" branded networking equipment from hundreds of different eBay and Amazon vendors, and does not consistently take any steps to vet those vendors, and Dexon's "haphazard approach to vendors" "creates an unacceptable risk that Dexon will procure counterfeit products." *See id.*, ¶¶ 102-108. As an example, LaMagna states Dexon has bought from companies (including an eBay account), one of which was associated with an individual who pleaded guilty to selling hundreds of millions of dollars of counterfeit equipment. *See id.*, ¶ 108.

In other adjacent paragraphs Dexon does not challenge, LaMagna explains that Dexon does not consistently inspect "Cisco" products before sending those products to customers. *See id.*, ¶¶ 110-116. In many cases, Dexon never takes physical possession of the product. Instead, "Dexon 'blind' or 'drop' ships products directly from its suppliers to Dexon's customers." *Id.*, ¶ 110.

declared that “Dexon would be unable to avoid the risk of unknowingly and unintentionally violating an injunction prohibiting the sale of counterfeit product.”

119. Unsurprisingly, the record evidence shows that Dexon has sold counterfeit “Cisco” products regularly. Indeed, multiple employees testified that Dexon keeps “suspect” equipment in at least three “quarantine locations” in Dexon’s office (also referred to internally as “purgatory” or “limbo”). For example, Kaas keeps “a fair amount of problematic equipment in his tech room,” including more than 20 switches that produced ILET errors. O’Neil keeps a pile of “allegedly problematic equipment” on the floor of his office, including “seven SFPs [transceivers] returned from a customer, and a switch alleged to be counterfeit.”

120. O’Neil also testified that the FBI raided Dexon’s offices in 2008 because it suspected Dexon was selling counterfeit products. According to documents from that investigation, 24 of 28 supposedly “Cisco” products that were provided to the FBI and Cisco were in fact determined to be counterfeit.

121. I understand that Dexon has continued to sell counterfeit networking equipment in the years since the raid the FBI conducted in 2008. The following are a few of the dozens of incidents of Dexon sales of counterfeit products that I understand the record to reflect:

- In 2015, Dexon sold “Cisco”-branded switches to Park Place Dealership in Texas. After certain switches that Dexon sold the dealership malfunctioned in 2018 and 2019, the customer contacted Cisco for support. Cisco’s engineers examined several of the products and determined that they were counterfeit. In this incident, a Dexon salesperson submitted a service request to Cisco’s TAC using his personal email address, attempting to procure a replacement for the counterfeit switches at Cisco’s expense.
- Also in 2015, Dexon sold a “Cisco”-branded 2960X-series switch to Things Remembered, Inc. After Things Remembered, Inc. contacted Cisco for assistance in 2020 because the switch had failed, Cisco engineers determined that the switch was counterfeit.
- In 2016, Dexon sold twenty “Cisco”-branded switches to Eastern New Mexico University. In August 2019, after one of the switches failed, Eastern New Mexico University contacted Cisco for technical support. Cisco engineers determined that the switch was counterfeit.
- In 2017, Dexon sold several “Cisco” 2960X-series switches to DZSP 21, LLC, a contractor for the U.S. Navy. After several counterfeit units appeared in the Navy’s infrastructure, federal law enforcement officials with Immigration and Customs Enforcement sought Cisco’s assistance in determining the source of these products. Cisco determined that at least four of those switches were counterfeit.

- In 2018, Dexon sold a “Cisco” 2960X-series switch to Community Health Alliance in Nevada. The customer contacted Cisco for assistance in 2020 after that switch malfunctioned. Upon further investigation, Cisco determined that this switch was counterfeit.
- In 2018, Dexon sold several “Cisco” 2960X-series switches to Lockridge Grindal Nauen in Minneapolis, Minnesota. Cisco was contacted for assistance in 2019 after several switches malfunctioned. Upon further investigation, Cisco determined that six switches were counterfeit.
- In July 2019, Dexon sold several “Cisco” GLC-TE series transceivers to Medrisk in King of Prussia, Pennsylvania. After the customer contacted Cisco for technical support, Cisco determined that eight transceivers were counterfeit.
- In September 2019, Dexon sold several “Cisco” QSFP series transceivers to Coppell Independent School District in Texas. After the customer contacted Cisco for technical support, Cisco determined that three of the transceivers were counterfeit.

122. I understand that, in most of these incidents, Dexon’s sales of counterfeit products came to Cisco’s attention only because customers who were under the false impression that they had purchased valid Cisco SMARTnet support from Dexon contacted Cisco to obtain support. Therefore, the incidents of Dexon-sold counterfeits reflected in the record likely understate the true extent of Dexon’s sales of counterfeit “Cisco” equipment.

123. Dexon has continued to sell counterfeit equipment despite multiple red flags that it is selling counterfeit products. Dexon has continued to purchase networking products at rock-bottom prices, despite being warned that such prices are “too good to be true” but instead are telltale signs of counterfeit networking equipment. Dexon has also continued to purchase from suppliers that UNEDA and other networking equipment resellers have explicitly warned Dexon are known for selling counterfeit equipment.

Id., ¶¶ 118-23 (internal footnotes omitted).

Dexon also moves to exclude three rebuttal opinions from his reply report, each of which references information LaMagna received from Cisco’s engineers as a basis for his opinions that Dexon sold counterfeit products:

Second, Ms. Mosteller claims that Cisco’s counterfeit determinations are “vulnerable to misidentifying authentic products as counterfeit.” Mosteller Rebuttal

¶¶ 58-59. She asserts that there is an unacceptable risk of human error because engineers manually input some product information. However, I understand that Cisco has implemented a two-level review process to reduce the risk of human error. First, the “test” specialist identifies and documents multiple product attributes that show the product is counterfeit. Second, the “validation” specialist independently verifies the test specialist’s findings. This two-level review process is reflected on an ESR, which states the names of the test and validation specialists. Furthermore, **according to my interviews with Mr. Heidecker and Mr. Ho, the authentication process, which relies largely on scientific inputs and outputs, is not a subjective process – a device is either authentic or it is counterfeit.** Getting all of the secure authentication features right is a significant challenge for counterfeiters.

...

For example, in August 2021, a large state university experienced problems with defective network modules and opened a case with Cisco’s Technical Assistance Center (TAC). Cisco asked the customer “where [it] purchased these from” and noted that “they are not up to Cisco manufacturing standards.” Dexon instructed: “If you could continue with trying to RMA [i.e., return and replace] these with Cisco, it would be appreciated. I’d suggest telling them that you are not sure where you purchased them, and weren’t able to locate a sale order number.” **Cisco engineer Mr. Ho concluded that the Dexon-sold modules were counterfeit.**

As another example, in October 2022, Cisco emailed the “energy company headquartered in Texas” referenced in Dexon’s Amended Complaint (Targa Resources) that **its engineers had determined that a switch Dexon sold the energy company was counterfeit.** Cisco urged the company to remove the switch from its network and requested vendor information. The customer forwarded that request to Dexon, and Dexon instructed: “Just ignore the request for vendor information as it won’t help you any.”

Id., ¶¶ 75, 96-97 (internal numbering and footnotes omitted omitted) (emphasis added).

When asked during his deposition if he confirmed whether Cisco’s findings were accurate with respect to counterfeit findings, LaMagna testified that he “took it on . . . face value that if Cisco says one of their products is counterfeit and their experts all agree on that, then I take it that they’re competent to make that determination.” Dkt. No. 330-4 (“LaMagna Dep. Tr.”) at 303:3-13; *see also id.* at 313:7-12 (“I did not delve into [Cisco’s] technical procedures, but given the fact that these are well-trained, experienced individuals and their procedures in my opinion are . . .

more than acceptable, . . . I took it on face value that their determination of counterfeit was accurate.”)).

2. Dexon’s assertions

Dexon argues LaMagna’s opinions are not reliable under *Daubert* because LaMagna does not possess the “technical knowledge about product authentication” or “expertise” necessary to determine whether the specific Cisco products sold by Dexon were in fact counterfeit. Dkt. No. 330 at 4; *see also id.* at 6 (citing *Bridgelux, Inc. v. Cree, Inc.*, 2008 WL 5549448, at *3-4 (E.D. Tex. Aug. 20, 2008) (excluding testimony that was outside the scope of the witness’s expertise)). Relying on LaMagna’s reports and deposition testimony, Dexon claims LaMagna, who is not an engineer, admittedly defers to those Cisco engineers with the “expertise” for those subjects. *Id.* at 6. According to Dexon, LaMagna does not state in either report that he independently confirmed Cisco’s findings that Dexon, despite its anti-counterfeiting measures, sold counterfeit networking equipment repeatedly; he does not explain how Cisco purports to examine products for counterfeit (including the tools used); and he does not explain how Cisco employees determined whether products sold by Dexon were purportedly counterfeit. *Id.*

Because LaMagna performed no independent analysis as to whether products sold by Dexon were counterfeit and because LaMagna lacks the technical expertise to either perform that analysis or confirm an existing analysis, Dexon claims that LaMagna will do nothing more than “parrot[] facts to the jury” or give “an argumentative summary of the evidence.”⁴ *Id.* at 5, 7. Dexon argues LaMagna’s “opinions simply repeat statements in Cisco documents and off-the-record

⁴ Defendants disagree, asserting LaMagna “reached each of his opinions based on his decades of experience in brand protection and anticounterfeiting.” Dkt. No. 346 at 11. According to Defendants, LaMagna considered not only Dexon’s purported sales of counterfeit, but also his own knowledge and experience of how effective anticounterfeiting programs are structured and the vulnerabilities that counterfeiters are likely to exploit. *Id.* (citing LaMagna Opening Report, ¶¶ 50, 54-57, 72-73, 74-78, 103, 106, 115-16; LaMagna Reply Report, ¶¶ 69-70, 72, 79, 85, 89).

conversations LaMagna had with Cisco employees” Michael Heidecker and Fookwai Ho; therefore, LaMagna’s challenged opinions risk “improperly usurping the function of the jury.” *Id.* at 1. Asserting the jury is just as capable as LaMagna in evaluating the evidence and determining whether products sold by Dexon were in fact counterfeit, Dexon contends LaMagna’s narrative testimony regarding the same should be excluded. *Id.* at 7.

3. Analysis

In the specific paragraphs challenged by Dexon, LaMagna opines that the inadequacy of Dexon’s anti-counterfeiting measures to protect against the sale of counterfeit products is bolstered by LaMagna’s review of the evidence showing that – despite Dexon’s anti-counterfeiting measures – Dexon has never detected a counterfeit “Cisco” product and has sold counterfeit networking equipment repeatedly. *See, e.g.*, LaMagna Opening Report, ¶¶ 88, 117. LaMagna then recites that evidence. Some of the evidence came from Dexon documents and employees’ testimony. *Id.*, ¶¶ 118-21; *see also* LaMagna Reply Report ¶ 71 (stating his opinions are based on his training and experience, as well as information he received during interviews with “Cisco product-authentication specialists Michael Heidecker and Fookwai Ho”). Some of the evidence was testimony regarding the FBI’s 2008 raid of Dexon’s offices wherein the FBI found counterfeit products. LaMagna Opening Report, ¶ 120; *see also* Dkt. No. 346-4 (O’Neil Dep. Tr.) at 164:15-165:9 (confirming that the FBI determined that some of the products taken from Dexon were potentially counterfeit).

The salient issue is whether it is improper for LaMagna—who does not claim to have the technical knowledge or skills required to determine whether products are counterfeit—to recite deposition testimony, Cisco’s documents, and off-the-record interviews with “Cisco product-authentication specialists” Heidecker and Ho, as support for LaMagna’s unchallenged opinion that

Dexon's anti-counterfeiting measures are inadequate to detect and avoid the trafficking of counterfeit equipment.

Defendants do not dispute that LaMagna is not qualified to determine (himself) if "Cisco" products are counterfeit, but argue it is a "common practice in brand protection" for experts to rely on "qualified specialists to authenticate goods," especially when the product is a "high-technology product (such as a switch or router)." Dkt. No. 346 at 9 (citing LaMagna Reply Report, ¶ 69) (stating that at Microsoft he relied on teams of product-authentication specialists to issue final determinations regarding the authenticity of Microsoft products). According to Defendants, Dexon's own brand protection expert, Mosteller, has relied on brand owners to authenticate technologically sophisticated products. *See* Dkt. No. 346-3 (Mosteller Dep. Tr.) at 31:8-32:15 (stating there were people at Revision who were able to test products to determine if they were authentic and further stating she did not personally conduct testing), 107:2-13, 109:1-110:10 (stating Revision ran a ballistic test on the goggles to determine that they were counterfeit and further stating she does not have "the expertise to run the type of tests that they ran or the equipment"), 112:11-116:1 (stating the individual that ran the tests would testify regarding the tests and that she trusted the individual that ran the tests at Revision to run them correctly). During her deposition, Mosteller agreed that Cisco "ha[s] the ability to identify counterfeit of [its] products." *Id.* at 242:15-18.

Defendants further point out that law enforcement agencies have relied on Cisco's product-authentication specialists to identify counterfeit "Cisco" products. *See* Dkt. No. 346 at 9 (citing LaMagna Reply Report, ¶ 70). Additionally, Defendants cite to a recent preliminary injunction order against Dexon in the California Litigation, stating the California court reviewed much of the same evidence that LaMagna did – including "engineering reports" from Cisco's product-

authentication specialists determining that products Dexon sold were counterfeit – and concluded that this evidence “demonstrates that Dexon has sold counterfeit Cisco products.” Dkt. No. 364 at 4 (quoting Dkt. No. 346-5 at 7, 9; also citing *id.* at 8 (“Cisco submitted a declaration from its global engineering manager, Michael Heidecker, who asserts that Cisco engineers have determined that hundreds of Cisco products sold by Dexon are counterfeit.”) (emphasis added by Defendants)).

Dexon has not shown that LaMagna improperly relies on information from Cisco’s product-authentication specialists (and similar sources) to identify counterfeit “Cisco” products as evidence in support of his opinions regarding the sufficiency of Dexon’s purported anti-counterfeiting measures. Both side’s experts acknowledge brand protection personnel rely on specialists to determine the authenticity of specific products. Nor has Dexon shown that LaMagna’s testimony as to purported counterfeit Dexon-sold goods would be unhelpful to, or usurp the function of, the jury. Whether Dexon has sold counterfeit goods could be helpful to the jury to evaluate LaMagna’s opinions, and Dexon remains free to challenge those opinions on cross.

Lamagna has clarified he is relying on Cisco engineer’s conclusions that Dexon sold counterfeit products—not his own analysis. Cisco also concedes that LaMagna is not an engineer and is not qualified to perform the tests that determine whether a specific product is counterfeit. As long as his testimony is consistent with those representations (*i.e.*, that *he* has not individually determined the authenticity of Dexon-sold products were counterfeit, but rather explaining that other purportedly qualified people made that determination), Dexon’s complaint is limited to the basis for LaMagna’s opinions. Questions relating to the bases and sources of an expert’s opinion generally affect the weight to be assigned to that opinion rather than its admissibility. *See* FED. R. EVID. 702 Advisory Committee’s Notes, 2000 Amendments (citing *Rock v. Arkansas*, 483 U.S. 44, 61 (1987)).

Further, experts may rely on contested facts (such as the accuracy of Cisco's own counterfeit determinations) and not usurp the function of the jury when doing so. *Pipitone v. Biomatrix, Inc.*, 288 F.3d 239, 249-50 (5th Cir. 2002) (noting that when facts are in dispute, experts sometimes reach different conclusions based on competing versions of the facts and concluding that the fact-finder was entitled to hear the doctor's testimony and decide whether it should accept or reject that testimony after considering all factors that weigh on credibility, including whether the predicate facts on which the doctor relied were accurate). Indeed, as urged by Defendants, factual disagreements are fodder for cross-examination, not exclusion *See* Dkt. No. 346 at 2 (citing *Mathis v. Exxon Corp.*, 302 F.3d 448, 461 (5th Cir. 2002)). As long as LaMagna is clear he has not personally conducted or verified the counterfeiting testing, and that he is relying on Cisco's own determination in that regard, the better course is to allow a thorough cross-examination.⁵ Dexon may approach the bench if it feels LaMagna crosses that line to suggest he personally made the determination that the cited products were counterfeit. The Court denies Dexon's motion to exclude LaMagna's opinions regarding purported counterfeit products sold by Dexon.

B. LaMagna's opinions comparing Cisco's brand protection practices with those of other networking manufacturers (LaMagna Opening Report at 5, ¶¶ 52, 54, 73, 81-86; LaMagna Reply Report, ¶¶ 14, 48-49, 69)

1. Challenged opinions

In the challenged sections of his reports, LaMagna opines (often in the same paragraph) that both Cisco's brand protection policies and practices are consistent with "best practices" and with those of other manufacturers of networking equipment. *See, e.g.*, LaMagna Opening Report at 5 ("Cisco's brand-protection policies and practices are consistent with best practices and those of other manufacturers of networking equipment, such as Juniper and HPE."). Other paragraphs

⁵ This ruling holds LaMagna's opinions on counterfeiting do not violate the *Daubert* standard. However, his testimony regarding counterfeiting must still comply with any forthcoming pretrial rulings and *limine* orders on that issue.

compare his experience at Microsoft to the networking industry. *See, e.g., id.* ¶ 52. However, Dexon’s motion seeks only to exclude LaMagna’s opinions comparing Cisco’s brand protection practices with those of other networking manufacturers. *See* Dkt. No. 330 at 7 (“LaMagna’s Opinions Comparing Cisco’s Brand Protection Practices With That of Other Networking Manufacturers Should be Excluded.”); *see also* Dkt. No. 349 at 4, n.4 (“The crux of Dexon’s challenge on this score is that LaMagna lacks the expertise and experience to offer an opinion as to whether Cisco’s brand protection practices are consistent with those of other networking manufacturers. Put differently, given his inexperience in the industry, LaMagna cannot offer an opinion as to how other networking manufacturers enforce their brand protection-centric policies.”).

2. Dexon’s assertions

Dexon moves to exclude LaMagna’s opinions comparing Cisco’s brand protection “practices” with those of other networking manufacturers as unreliable, asserting they are not based on facts, evidence, or data. Dkt. No. 330 at 7-8. Specifically, Dexon asserts as follows:

In both his Opening and Reply Reports, LaMagna discusses Cisco’s brand protection practices in comparison with other networking brands—such as Dell, Juniper, HPE, Arista Networks, NETGEAR, and Extreme Networks. (LaMagna Opening Report, ¶¶ 81-85); LaMagna Reply Report, ¶¶ 14, 48). Specifically, LaMagna relies upon warranty and support contracts, channel partner agreements, and end-user license agreements that are publicly available on other networking manufacturing brand websites. (*Id.*). LaMagna then infers that because Cisco’s contracts, agreements, and policies are similar to that of other brands in the networking industry, then Cisco’s brand protection *practices* must be consistent with the industry norm. (*See* LaMagna Opening Report, ¶ 81 (“I have reviewed the policies of other networking-equipment manufacturers regarding warranty entitlement, gray market products, and anti-counterfeiting measures. I conclude that Cisco’s practices are consistent with those of other manufacturers.”); LaMagna Reply Report, ¶ 48 (“The practices of other networking-equipment manufacturers confirm that end-user software-compliance audits are an accepted practice among networking-equipment.”)). These conclusions are unsupported.

Id. at 8 (emphasis original).

3. Analysis

As explained below, the Court grants Dexon's narrow request and excludes LaMagna's opinions on how Cisco's brand protection practices are consistent with the practices of other companies in the networking industry. However, the Court does not exclude any opinions contained in the challenged paragraphs that Cisco's brand protection policies are similar to or consistent with (1) programs like the one LaMagna developed at Microsoft or (2) the policies of other manufacturers of networking equipment.

In evaluating Cisco's Brand Protection program and concluding it is consistent with "best practices" in brand protection, LaMagna compared Cisco's policies and agreements to those of other networking-equipment manufacturers. LaMagna concluded that Cisco's policies concerning "gray market" products, warranties, and/or agreements with authorized resellers and end-users are consistent with those of Cisco's competitors, such as Dell, Juniper, HPE, Arista Networks, NETGEAR, Extreme Networks, Palo Alto Networks, and VMWare. LaMagna Opening Report, ¶¶ 81-85. For example, like Cisco, HPE provides that warranties are only "available to original bona fide end users who purchased th[e] product through an authorized HPE distribution channel," *see* LaMagna Opening Report, ¶ 82 (quoting policy), and Juniper similarly provides that "gray market" goods are only eligible for service upon payment of an inspection and reinstatement fee. *See id.*, ¶ 83 (citing policy). As noted above, in the challenged sections of his reports, LaMagna opines that both Cisco's brand protection policies *and* practices are consistent with "best practices" and those of other manufacturers of networking equipment. LaMagna Opening Report at 5.

While LaMagna may testify about the similarity between brand protection policies across the networking industry, he does not have a sufficiently reliable basis to infer Cisco's practices are consistent with those of other companies. That opinion is formed by simply reviewing information

made publicly available online, and there has been no evidence presented to support LaMagna's "inference" that other networking manufacturers enforce brand protection enforcement in the same manner as Cisco. Dkt. No. 349 at 5.

Both parties acknowledge LaMagna's opinion is based on that "inference." *See* Dexon's motion (Dkt. No. 330) at 8 ("LaMagna relies upon warranty and support contracts, channel partner agreements, and end-user license agreements that are publicly available on other networking manufacturing brand websites. . . . LaMagna then infers that because Cisco's contracts, agreements, and policies are similar to that of other brands in the networking industry, then Cisco's brand protection *practices* must be consistent with the industry norm.") (emphasis by Dexon); *see also* Defendants' response (Dkt. No. 346) at 14 (arguing this "reasonable inference" is supported by LaMagna's expertise and experience in brand protection). However, LaMagna has not worked with networking companies such as Dell, Juniper, Arista Networks, NETGEAR, and Extreme Networks, Dkt. No. 330-4 (LaMagna Dep. Tr.) at 232:15-233:13, and he has never spoken to any of these companies about their brand protection programs. *Id.* at 233:21-234:14. LaMagna admits he based his opinions on what these companies "published as their policies and procedures and practices." *Id.* at 236:16-18.

This "inference" concerns too crucial an issue in the case to allow LaMagna to offer such an opinion based on so little support. The issue of whether Cisco *applies* its brand protection policies in an anticompetitive way is a central dispute in the case. *See, e.g.*, Dexon's response to Cisco's summary judgment motion (Dkt. No. 355) at 10 (Dexon stating that despite similar policies, "there is no evidence that any networking company apart from Cisco employs similar FUD or intimidation tactics with its customers."); *see also id.* at 21 (Dexon explaining its theory that "what makes Cisco's audits anticompetitive is the manner and circumstances in which they

are carried out” (emphasis by Dexon)); Dkt. No. 397 (Transcript) at 103:16-104:14 (Dexon explaining it is not challenging Cisco’s policy of not “putting SmartNet on unauthorized [equipment]” but how Cisco allegedly applies that policy resulting in a “bait and switch”). Given the importance of that issue, LaMagna would need a more reliable basis than a “reasonable inference” to conclude that just because Cisco’s policies are similar to the other networking equipment manufacturers, its *practices* of implementing those policies must also be similar. But he does not offer experience in the networking industry or provide an analysis of how other companies implement their policies that would assist the jury in comparing Cisco’s practices to those of other networking companies.

The admission or exclusion of expert witness testimony is a matter that is left to the discretion of the district court. *See, e.g., United States v. Herman*, 997 F.3d 251, 269 (5th Cir. 2021), *cert. denied*, 142 S. Ct. 787, 211 L. Ed. 2d 490 (2022) (“This court reviews ‘the district court’s decision to exclude expert witness testimony under an abuse of discretion standard, and the ruling will not be disturbed on appeal unless it is *manifestly erroneous*.’”); *see also Seatrax, Inc. v. Sonbeck Int’l, Inc.*, 200 F.3d 358, 371 (5th Cir. 2000). The Court, in its discretion, excludes LaMagna’s opinions that Cisco’s brand protection “practices” are consistent with the “practices” of other manufacturers of networking equipment.

IV. CONCLUSION

Based on the foregoing, it is

ORDERED that Dexon Computer Inc.’s *Daubert* Motion to Exclude Opinions of Richard LaMagna (Dkt. No. 330) is **GRANTED IN PART and DENIED IN PART**.

The Court excludes LaMagna's opinions to the extent they opine that Cisco's brand protection practices are consistent with the practices of other manufacturers of networking equipment. Dexon's motion is otherwise denied.

SIGNED this the 18th day of December, 2023.



J. Boone Baxter
UNITED STATES MAGISTRATE JUDGE